# Event-trigger Based Resilient Distributed Energy Management Against FDI and DoS Attack of Cyber-Physical System of Smart Grid

Huifeng Zhang, *Senior Member, IEEE,* Zhuxiang Chen, Chengqian Yu, Dong Yue, *Fellow, IEEE,* and Xiangpeng Xie, *Senior Member, IEEE,* Gerhard P. Hancke, *Life Fellow, IEEE*

***Abstract*—To address the false data injection (FDI) and denial of service (DoS) attack, this paper proposes an event-trigger based resilient distributed energy management approach for cyber-physical system of smart grid. Here, an event-trigger based resilient consensus algorithm (ERCA) is proposed with attack identification and compensation mechanism. The event-triggered mechanism is improved within distributed optimization combined with reliable acknowledgment (ACK) signals technique to mitigate the impact of data loss or transmission delay, and trust nodes based compensation approach is proposed during resilient coordinated optimization for state correction to ensure the stability and security of power grid system. The optimality and convergence of proposed method is proved theoretically that the proposed method can approximate to optimal solution well and achieve consensus by ensuring the proactive involvement of all participants under coordinated cyber attack. According to those obtained simulation results, it reveals that the proposed algorithm can effectively solve the energy management issue under coordinated DoS and FDI attack.**

***Index Terms*—Energy management, false data injection, denial of service, event-triggered, resilient consensus algorithm**

## NOMENCLATURE

*Abbreviations*

| | |
|---|---|
| FDI | False Data Injection |
| ACK | Acknowledgment |
| DoS | Denial of Service |
| CPS | Cyber-Physical Systems |
| LFC | Load Frequency Control |

H. Zhang is with the Institute of Advanced Technology, Nanjing University of Posts and Telecommunications, Jiangsu Province, China, 210023, e-mail: zhanghuifeng_520@163.com (Corresponding author)

Z. Chen is with the Institute of Advanced Technology, Nanjing University of Posts and Telecommunications, Jiangsu Province, China, 210023, e-mail: chenzhuxiang99@163.com

C. Yu is with the Institute of Advanced Technology, Nanjing University of Posts and Telecommunications, Jiangsu Province, China, 210023, e-mail: 1222056208@njupt.edu.cn

D. Yue is with the Institute of Advanced Technology, Nanjing University of Posts and Telecommunications, Jiangsu Province, China, 210023, e-mail: medongy@vip.163.com (Corresponding author)

X. Xie is with the Institute of Advanced Technology, Nanjing University of Posts and Telecommunications,Jiangsu Province, China, 210023, e-mail: xiexiangpeng1953@163.com

G. P. Hancke is with the College of Automation, Nanjing University of Posts and Telecommunications,Jiangsu Province, China, 210023, and also with the Department of Electrical, Electronic and Computer Engineering, University of Pretoria, South Africa, 0002, e-mail: g.hancke@ieee.org

*Algebraic Symbols*

| | |
|---|---|
| $G$ | Undirected Graph |
| $a_{ij}$ | Doubly stochastic matrix |
| $A$ | Weight Matrix |
| $N_i$ | Neighbor node set |
| $V$ | Set of $n$ agents |
| $V_G$ | Distributed generators set |
| $V_D$ | Responsive demands set |
| $V_T$ | Trusted node set |
| $V_N$ | Normal node set |
| $V_M$ | Malicious node set |
| $E$ | Set of edges |
| B | Connected dominating set |
| $\eta$ | Feedback proportional parameter |
| $\alpha_k$ | Decay iteration step |
| $J(P)$ | Objective function |
| $J^{'}$ | Differentiable value |
| $H$ | Upper limit of the differential value $J^{'}$ |
| $\lambda_i$ | Incremental cost |
| $\xi_i(k)$ | Local mismatch power |
| $C_i\left(P_i\right)$ | Cost function of generator |
| $P_j^M(P_j^m)$ | Upper(Lower) bound of the load unit |
| $a_{0i}$,$a_{1i}$,$a_{2i}$ | Cost parameter |
| $U_j(P_j)$ | Utility function |
| $\tau_j$,$\partial_j$ | Satisfaction factors |
| $d_i\left(k\right)$ | Derivative of the objective function $J(P)$ |
| $L_i\left(k\right)$ | Triggering threshold |
| $D_{ij}\left(k\right)$ | Set of DoS attack nodes |
| $F_i\left(k\right)$ | Set of FDI attack nodes |
| $S_i\left(k\right)$ | Set of secure nodes |
| $\varphi$ | Random communication loss rate |
| $w_{ij}$ | Row random matrix |
| $W(k)$ | Weight Matrix |
| $\Phi(k,t)$ | Inverse product |
| $Y(\mu,\nu)$ | Optimal convex set |
| $\theta_i\left(k\right)$ | State error |
| $\Pi\left(t\right)$ | Random vector |
| $t_{ack}$ | Communication time |
| $t_M$ | Maximum delay time |
| ${\lambda_i}^{M(m)}\left(k\right)$ | Maximum/Minimum states |
| $v_i^{\lambda}$ | False value |
| $\widehat{e}_i(k)$ | Correction variable |

## I. Introduction

SMART grid is a power system based on information technology and communication technology, which can monitor, control, and optimize the various components of the power system in real-time. Energy management is an important part of smart grid. By optimizing the collection, storage, conversion, and utilization of energy, energy management can achieve efficient energy use, reduce energy consumption and emissions, improve energy utilization efficiency, support the application of new energy technologies, and attain sustainable energy development [1]. With the development of clean energy and the limited ability of centralized energy supply regulation, distributed architectures are widely used due to their flexible energy supply and high energy utilization [2], [3]. Meanwhile, traditional network control systems heavily rely on conventional technologies, while cyber-physical systems (CPS) integrate physical processes, communication networks, and enabling massive computing, precise control, and autonomous coordination. Currently, CPS are widely applied in smart grids, smart healthcare, and transportation systems [4]. The rapid development of digital communication and modern technology has provided opportunities for malicious node attacks on CPS. Among them, FDI attacks and DoS attacks are the most prevalent. Usually, FDI attacks inject false information into the power system by tampering with data, destroying the accuracy of system data. DoS attacks affect the power system with numerous irrelevant requests, resulting in communication disruption, data loss, and impacting real-time data transmission. Obviously, both attacks affect the reliability and security of the power grid, leading to inaccurate and unreliable energy distribution and management. Therefore, appropriate network security measures must be taken to ensure the safety of smart grid.

There have been many studies on FDI attacks [5]–[9]. In [5], a strategy is presented for resilient distributed secondary control in island microgrids, aiming to ensure frequency synchronization and recovery. This method employs a hidden layer-based attack elastic control scheme, designed to counteract FDI attacks targeting secondary control system components like actuators, sensors, and communication links. Cai et al. [6] introduce a resilient distributed Nash Equilibrium search algorithm that possesses resilient properties, allowing the system to converge towards network elements even information about the characterization of FDI attacks is missing. For network multi-group systems, [8] provides a completely distributed and resilient control approach, including the original network physical layer and virtual elastic layer. This methodology is designed to effectively address unforeseen and unlimited FDI attacks. Guo et al. [9] designs an FDI attack scheme, taking into account real-world physical scenarios. It crafts a forward channel attack signal to achieve the stealthiness of FDI attacks. In addition, there are also many research achievements on DoS attack [10]–[17]. Reference [11] proposes a novel detection method based on Deterministic Probabilistic Automaton, capturing anticipated states to detect malicious attacks during the communication process in smart grids. In [15], the article delves into the challenge of network security control when faced DoS attacks, particularly focusing on equalization and voltage restoration within isolated DC microgrids. The study introduces a resilient sampling mechanism that aims to achieve the restoration of bus voltage. Li et al. [17] tackle data loss caused by DoS attacks by utilizing latest measurement packets. They enhance the performance of traditional state estimation algorithms by integrating Holt's two-parameter exponential smoothing and extended Kalman filtering techniques. In addition, event triggered mechanisms are actively used in resilient methods to reduce the communication burden [18]–[21]. Lu et al. [18] have established a new switching LFC system model based on the event-triggered communication strategy, aiming to reduce the communications burden and guarantee network security. In Ref [21], a fresh event-triggered framework was proposed by introducing the concept of "triggering domain", which relieved the communication burden and meanwhile maintains the desired secure filtering performance for the switched CPSs. Currently, existing resilience strategies for studying both DoS and FDI attacks [22], [23] are limited. Guo et al. [23] relies on an event-triggered mechanism to build a switch-state feedback controller to ensure system stability under attack. However, most existing methods only target individual attacks and lack scalability, few methods have been applied in energy management of smart grid. Therefore, this paper focuses on cyber-physical system and proposes an event-triggered resilient consensus strategy with an attack detection mechanism. This strategy is designed to address the impact of FDI and DoS attacks on power systems, ensuring the security and efficiency of smart grids. The main contributions of this work can be outlined as follows:

1) To address the DoS attack, event-triggered mechanism based distributed optimization method is improved with reliable ACK signals technique, which can detect the transmission state of participant information. The improved method can mitigate the impact of data loss or transmission delay.
2) Due to the security risks posed by FDI attack, a compensation mechanism is proposed during the coordinated optimization on the basis of trust nodes based distributed energy management approach, it can correct the abnormal state with trust nodes identification technique, which can be more scalable and stable in comparison to those existing methods.
3) The convergence of proposed approach have been theoretically proved, and simulation results on IEEE 39-bus system also reveal that the proposed method can tackle with the energy management of power cyber-physical system under DoS and FDI attack.

The subsequent sections can be organized as: Section II establishes the system model and introduces the FDI and DoS attack models. Section III outlines the primary resilient algorithms. Section IV presents theoretical analysis, while Section V showcases simulation outcomes validating the algorithm's

reliability, and Section VI concludes the whole work.

## II. PROBLEM FORMULATION AND PRELIMINARIES

### A. Communication Network Model

The network of power grid formed by various generators and loads, can be conceptualized as an undirected graph. The communication network can be described with an undirected graph $G = \{V, E\}$, where $V$ represents a set of $n$ agents, consisting of distributed generators set $V_G$ and responsive demands set $V_D$, $E \subset V \times V$ is the set of edges. For an undirected graph, any edge $(V_i, V_j) \in E$ also has a corresponding edge $(V_j, V_i) \in E$. The neighbor node set of each node $i$ is defined as $N_i = \{j | j \in V, (i,j) \in E, j \neq i\}$. This article does not consider self-loops, i.e.,$(i,i) \notin E, \forall i \in V$. Additionally, a weight matrix $A = [a_{ij}] \in R^{n \times n}$ is defined to describe the connectivity between nodes. If the weight matrix $A$ is row or column stochastic, this means that either $\sum_{i=1}^{n} a_{ij} = 1$ or $\sum_{j=1}^{n} a_{ij} = 1$; if it is double stochastic, both $\sum_{i=1}^{n} a_{ij} = 1$ and $\sum_{j=1}^{n} a_{ij} = 1$ hold simultaneously. Here, it defines a doubly stochastic matrix $A$:

$$a_{ij} = \begin{cases} \frac{1}{|N_i|+1}, & j \in N_i \\ 1 - \sum_{j \in N_i} a_{ij}, & j = i \\ 0, & j \neq i \end{cases} \tag{1}$$

Meanwhile, all nodes in the undirected graph are classified into three types as:

- Trusted nodes: Investing more resources on trusted nodes to enhance their security and make them less susceptible to attacks, trusted node set is noted as $V_T$.
- Normal nodes: Normal nodes can recognize information about its neighbors and perform iterations. However, it can be infected by attackers, normal node set is noted as $V_N$.
- Malicious nodes: Malicious nodes can obtain information from their neighbors, maliciously modify the neighbor's information, and disrupt the iteration of normal nodes, malicious node set is noted as $V_M$.

The concept of connected dominating set is refereed in literature [24].

**Definition 1:** The set $\mathrm{B} \subset G$ is called as a connected dominating set if arbitrary node $i \notin \mathrm{B}$ has at least one neighbor node $j$ that satisfies $j \in \mathrm{B}$, and all those nodes in set B can form a connected graph.

**Assumption 1:** All trusted nodes can form a connected dominating set of $G = \{V, E\}$.

### B. Physical System Model

In a smart grid, the main task of energy management involves minimizing costs associated with each generation and load unit within a certain time range and improve energy utilization efficiency with considering the balance between generation and load demand and several power/load limits. The specific problem is described as follows:

$$\min J(P) = \sum_{i \in V_G} C_i(P_i) - \sum_{j \in V_D} U_j(P_j) \tag{2}$$

where $C_i(P_i)$ is the cost function of generator $i (i \in V_G)$; $U_j(P_j)$ represents the utility function of each load $j (j \in V_D)$; $P_i$ and $P_j$ are the generation power of each generator unit $i$ and the demand power of each load unit $j$ respectively.

*1) The cost function for generator $i$:* The cost function $C_i(P_i)$ of each generation unit can be described as:

$$C_i(P_i) = a_{0i} P_i^2 + a_{1i} P_i + a_{2i} \tag{3}$$

where $a_{0i}$,$a_{1i}$,$a_{2i}$ is the cost parameter, $P_i^M$ and $P_i^m$ are the upper and lower limits of power generation, respectively. $C_i(P_i)$ maps the relationship between the generation cost and the generation quantity of each power generation unit $i$, where the quadratic cost term $a_{0i} P_i^2$ reflects variations in power efficiency as the generated electricity quantity increases, the linear cost term $a_{1i} P_i$ reflects operational cost, and the constant term $a_{2i}$ represents the fixed costs incurred during the power generation process.

*2) The utility function of the load:* The utility function $U_j(P_j)$ represents the degree of satisfaction with the electricity usage quantity $P_j$, it satisfies the following characteristics:

- $U_j(P_j)$ is a continuously derivable non-concave function.
- $U_j(P_j)$ is a non-decreasing function with a non-negative first derivative.
- $U_j(P_j) = 0$, it means that when no electricity is used, the satisfaction degree of the load unit is 0.

Therefore, a utility function $U_j(P_j)$ that satisfies the following condition as:

$$U_j(P_j) = \begin{cases} \tau_j P_j - \partial_j P_j^2, & P_j \leq \frac{\tau_j}{2\partial_j} \\ \frac{\tau_j^2}{4\partial_j}, & P_j > \frac{\tau_j}{2\partial_j} \end{cases} \tag{4}$$

where $\tau_j$ and $\partial_j$ are satisfaction factors, and the upper(lower) bound of the load unit is $P_j^M (P_j^m)$. The condition $P_j \leq \frac{\tau_j}{2\partial_j}$ reflects the consumer's decreasing utility perceptions, i.e., the user has a decreasing marginal utility as electricity consumption increases; If $\frac{\tau_j}{2\partial_j}$ is satisfied, the consumer has the maximum demand, and a further increase in electricity consumption will no longer improve the consumer's satisfaction. Therefore, the optimization problem for multiple generation units and load units can be described as:

$$\begin{aligned} &\min J(P) = \sum_{i \in V_G} C_i(P_i) - \sum_{j \in V_D} U_j(P_j) \\ &s.t. \sum_{i \in V_G} P_i = \sum_{j \in V_D} P_j \\ &P_i^m \leq P_i \leq P_i^M, i \in V_G \\ &P_j^m \leq P_j \leq P_j^M, j \in V_D \end{aligned} \tag{5}$$

it is assumed that the objective function $J(P)$ is continuously differentiable and Lipschitz continuous, and it satisfies that the differentiable value $J^{'} \leq H$, where $H$ is a constant. Thus, consensus-based algorithms can be described as:

$$\lambda_i(k+1) = \sum_{j \in V} a_{ij} \lambda_j(k) + \eta \xi_i(k) - \alpha_k d_i(k) \tag{6}$$

where $\lambda_i = 2a_{0i} P_i + a_{1i}$ is the incremental cost of the generation unit $i$, $\lambda_j = \frac{dU_j(P_j)}{dP_j}$ is the incremental utility of the load unit $j$, and $\xi_i(k)$ represents the local mismatch

power of node $i$, $\eta$ is the feedback proportional parameter with $0 < \eta < 1$, $\alpha_k$ is the decay iteration step and it satisfies Assumption 2 in literature [25], $d_i(k)$ is the derivative of the objective function $J(P)$.

**Assumption 2:** The decay iteration step $\alpha_k$ satisfies $\sum_{0}^{\infty} \alpha_k = \infty$, $\sum_{0}^{\infty} \alpha_k^2 < \infty$ and $\lim_{k\to\infty} \alpha_k = 0$, where $\alpha_k$ is designed to accelerate the convergence of $\lambda_i$ to the optimal value.

### C. Cyber Attack Model

*1) FDI Attack Model:* Attackers can hijack normal nodes and turn them into malicious nodes, which can import any false information in the state variables, denoted as $v_i^{\lambda}$. For convenience, it simulates the situation where the state variable $\lambda_i(k)$ is under FDI attack. The state variable can be modeled as:

$$\lambda_i(k+1) = \sum_{j\in V} a_{ij}\lambda_j(k) + \eta\xi_i(k) - \alpha_k d_i(k) + \tau v_i^{\lambda}(k) \tag{7}$$

where $v_i^{\lambda} \in R$ is an arbitrary value. If node $i$ is hijacked by an attacker, then $\tau = 1$, while $\tau = 0$ if it is a normal node. If the attacker just injects random data into the system, though the system convergence can be interrupted, it can be easily detected by the inspector. Here, it is assumed that the attacker can know some basic information of power system, but the generated FDI attack can still disrupt the stability and reliability of the power grid, which means that the FDI attack satisfies Lemma 1.

**Lemma 1:** When the attack injects false data satisfies [26]:

$$\lim_{k\to\infty} \tau v_i^{\lambda}(k) = 0, \sum_{k=0}^{\infty} \left|\tau v_i^{\lambda}(k)\right| \le \mathrm{Z}, i \in V \tag{8}$$

A stealthy attack is defined as $i \in V$:

$$\lim_{k\to\infty} \lambda_i(k) = \lambda^a, \lim_{k\to\infty} P_i(k) = {P_i}^a, \lim_{k\to\infty} \xi_i(k) = 0 \tag{9}$$

where Z, $\lambda^a$, ${P_i}^a$ are constant parameters.

*2) DoS Attack Model:* DoS attack can block the communication link between arbitrary node $i$ and its neighbor node $j$, which can result in the data loss between these two communication nodes. Typically, the random communication loss rate follows a Bernoulli distribution (binomial distribution) as [27]:

$$\begin{aligned} &\Pr\{\varsigma(k) = 0\} = \varphi \\ &\Pr\{\varsigma(k) = 1\} = 1 - \varphi \end{aligned} \tag{10}$$

where $\varsigma(k) = 1$ signifies successful broadcast, while $\varsigma(k) = 0$ represents failed communication, $\varphi$ denotes the packet loss rate between adjacent nodes, satisfying $0 < \varphi < 1$. Typically, the packet loss rate caused by DoS attacks is slightly higher than the random loss rate. If a DoS attack occurs on the communication path from node $i$ to $j$, the broadcast state of node $i$ is $\lambda_i(k+1) = 0$, as it fails to broadcast the data successfully.

## III. EVENT-TRIGGERED RESILIENT CONSENSUS UNDER CYBER ATTACK

### A. Detection of FDI and DoS Attack

For the purpose of monitoring participant state and mitigating the impact of DoS attacks, a secure and reliable acknowledgment(ACK) [28] signal is introduced in this paper. Node $i$ simultaneously transmits state information and ACK to its neighbor $j$. It is worth noting that ACK is assumed to be completely reliable and will not be lost. And the system cannot perform a timeout retransmission operation. During the communication window of $t_{ack} + t_M$, with $t_M$ denoting the maximum delay, successful transmission of state information is confirmed for node $i$ if it receives ACK from its neighbor. Conversely, failure to receive ACK marks the communication path from node $i$ to $j$ as disrupted. Therefore, setting $D_{ij}(k) = \{i | ij \in DoS\}\,(j \in N_i)$ represents the set of nodes that did not successfully broadcast information when the link between node $i$ and $j$ is disrupted by DoS attacks.

In addition, the state of the trusted node is the true trusted value, so the FDI attack is detected through trusted node screening. After node $i$ collects neighbor's information from its neighboring node $j$, it sorts the collected trusted node state and its own state to obtain the maximum/minimum states ${\lambda_i}^{M(m)}(k) = \max(\min)\{\lambda_j(k) | j \in \mathrm{V}_T \cup \{i\}\}$. When the state of a normal node exceeds $[\lambda_i^m(k), \lambda_i^M(k)]$, it is considered to be infected by the attacker, and therefore the set of nodes with abnormal states due to FDI attacks is designated as $F_i(k) = \{i | i \in FDI\}$. When the node's state is within the range, it is considered safe, and the set of secure nodes is denoted as $S_i(k) = \left\{i | \lambda_i^m(k) \le \lambda_i(k) \le \lambda_i^M, i \in N_i \cup \{i\}\right\}$.

### B. Resilient algorithm design under event-triggered mechanism

To enhance microgrid security and reliability, an elastic consistency algorithm is devised to alleviate the impact of potential attacks. Preceding this, an event-triggered mechanism is explored as a solution to the DoS attack concern. Initially, an auxiliary variable $e_i(k) = \lambda i(k) - \widehat{\lambda} i(k)$ is introduced, quantifying the error between the current updated state and the preceding triggered state. Furthermore, $T_i(k) = |e_i(k)| - Li(k)$ is defined, with $Li(k)$ representing the triggering threshold, which represents the maximum allowable error, and it should satisfy Assumption 3.

**Assumption 3:** For all $i \in V$,$j \in N_i$,$L_i(k)$ satisfies the following attributes:

$$L_i(k) \le L(k), \lim_{k\to\infty} L(k) = 0, \sum_{k=0}^{\infty} L^2(k) < \infty. \tag{11}$$

The condition for triggering the mechanism is $T_i(k) > 0$, where $k$ is the triggering time. If $T_i(k) > 0$, the event is triggered,at which point $\widehat{\lambda}_i(k) = \lambda_i(k)$, and node $i$ broadcasts the current state to neighboring node $j$, otherwise, $\widehat{\lambda}_i(k) = \widehat{\lambda}_i(k-1) = \lambda_i(k) + e_i(k)$. Therefore, a correction variable

$\widehat{e}_i(k)$ is defined to simplify the iteration process of the event-triggered mechanism.

$$\widehat{e}_i\left(k\right)=\begin{cases} e_i\left(k\right), T_i\left(k\right)<0 \\ 0, T_i\left(k\right)\geq 0 \end{cases} \tag{12}$$

where $\hat{e}_i(k)$ is the correction variable.

**Remark 1:** Assumptions 2 and 3 explain the nature of the decay iteration step and event triggering threshold, respectively, and according to literature [25], the preferred data format selected is $\frac{\iota}{(k+\rho)^o}$, where $\rho$ and $\iota$ are positive constants, and $0.5<o\leq 1$, at which point the trigger frequency and convergence rate can be effectively controlled.

Due to the information sharing among microgrids based on the event-triggered communication mechanism, when a DoS attack is detected, the event-triggered mechanism characteristic is utilized to update the state of the current moment based on the triggering state of the previous moment, ensuring the normal iteration of the microgrid. It is worth mentioning that nodes that fail to successfully send neighboring state values may also be subject to FDI attacks. Therefore, all participants need to rely on trusted nodes for abnormal state detection,all abnormal nodes are in the set $F_i\left(k\right)$. To correct the state caused by FDI attack, this paper proposes a new iteration algorithm for abnormal nodes, which relies on the average state of the max and min states of their neighboring trusted nodes to update their own states. Nodes within the safety set are updated by normal iterative states. Combining with the event-triggered mechanism, the state of each node at iteration $k$ is summarized as:

$$\widetilde{\lambda}_i\left(k\right)=\begin{cases} \widehat{\lambda}_i\left(k-1\right), i\in D_{ij}\left(k\right) \\ \widehat{\lambda}_i\left(k\right), i\in S_i\left(k\right) \\ \frac{\widehat{\lambda}_i^m(k)+\widehat{\lambda}_i^M(k)}{2}, i\in F_i\left(k\right) \end{cases} \tag{13}$$

The proposed algorithm firstly detects the state of each node and assigns it to a reasonable set, and then broadcasts the state $\widetilde{\lambda}_i\left(k\right)$ of all participants based on 15. At the same time, a row random matrix $w_{ij}=\frac{1}{|S_i+F_i|}$ is designed to solve the optimization problem. The consistency algorithm is rewritten as follows:

$$\begin{aligned}\lambda_i(k+1)=&\sum_{j\in S_i(k)}w_{ij}\widetilde{\lambda}_j(k)+\sum_{j\in F_i(k)}w_{ij}\widetilde{\lambda}_j(k)\\&+\tau v_i^{\lambda}\left(k\right)+\eta\xi_i(k)-\alpha_k d_i(k)\end{aligned} \tag{14}$$

Then the specific energy management procedures are described in Algorithm 1.

## IV. Convergence analysis of ERCA

With consideration of the effects of FDI and DoS attacks, this section validates the performance of ERCA. Some lemmas are required as follows, which is critical for the proof of the following convergence analysis.

**Lemma 2:** If the set of trusted nodes satisfies Assumption 1, the matrix form of Algorithm (14) can be written as:

$$\Gamma(k+1)=W(k)\Gamma(k)+\Delta(k)-\alpha_k d_k \tag{18}$$

**Algorithm 1** Event-triggered resilient consensus algorithm(ERCA)

**Initialization**: set $\lambda_i(0)$, $P_i(0)$, and $\xi_i\left(0\right)$,$i\in V$ as follows,

$$\lambda_i\left(0\right)=\begin{cases} {C_i}'\left(P_i^m\right), i\in V_g \\ {U_i}'\left(P_i^M\right), i\in V_d \end{cases}, P_i\left(0\right)=\xi_i\left(0\right)=0, \forall i\in V \tag{15}$$

set $\sigma_1$ and $\sigma_2$ as termination errors.

**Iteration:**Loop

Step 1. Revision of $\widetilde{\lambda}_i(k)$ is carried out by each node $i$ based on (13).

Step 2. Update of $\lambda_i(k+1)$ is performed by each node $i$ according to (14).

Step 3. Update of $P(k+1)$ is executed by each node $i$.

$$P_i\left(k+1\right)= \begin{cases} \underset{{P_i}^m\leq P_i(k)\leq P_i^M}{\arg\min}\left[C_i\left(P_i\left(k\right)\right)-\lambda_i\left(k+1\right)P_i\left(k\right)\right], i\in V_g \\ \underset{{P_i}^m\leq P_i(k)\leq P_i^M}{\arg\min}\left[\lambda_i\left(k+1\right)P_i\left(k\right)-U_i\left(P_i\left(k\right)\right)\right], j\in V_d \end{cases} \tag{16}$$

Step 4. Update of $\xi_i(k)$ is conducted by each node $i$.

$$\xi_i(k+1)= \begin{cases} \sum\limits_{j\in V}a_{ij}\widehat{\xi}_j\left(k\right)+P_i\left(k\right)-P_i\left(k+1\right), i\in V_g \\ \sum\limits_{j\in V}a_{ij}\widehat{\xi}_j\left(k\right)+P_i\left(k+1\right)-P_i\left(k\right), j\in V_d \end{cases} \tag{17}$$

**Until** $|\lambda_i(k+1)-\lambda_i|<\sigma_1$ or $|\xi_i(k)|<\sigma_2$ for all $i\in V$.
**Output** $\lambda_i$, $P_i$, and $\xi_i$, $i\in V$.

where weighting matrix $W(k)=[w_{ij}]_{N\times N}$, gradient vector matrix $d_k=[d_1\left(k\right),d_2\left(k\right),\cdots,d_N\left(k\right)]$, and state errors matrix $\Delta_k=[\Delta_1,\Delta_2,\cdots,\Delta_N]$. Especially, the state error of abnormal nodes are defined as $\theta_i\left(k\right)=\sum_{j\in F_i(k)}w_{ij}\left(\frac{\widehat{\lambda}_i^m(k)+\widehat{\lambda}_i^M(k)}{2}-\widehat{\lambda}_j\left(k\right)\right)$, where $\Delta(k)$ is bounded. It should be noted that the presence of state errors leads to differences in the proofs of Lemma 2 and [29], besides, the proof in this paper consider convergence for all participants.

Proof: The Lemma 2 can be proved in Appendix.A.

**Lemma 3:** If ERCA satisfies Assumption 1, any sequence $\Phi(k,t)$ satisfies the following nature [24]:

1) $\Phi(k,t)$ has $\lim_{k\geq t,k\to\infty}\Phi(k,t)=1\Pi(t)$, where $\Pi\left(t\right)\in R^N$ is a random vector related to $t$.

2) $\Phi(k,t)$ satisfies $|\Phi_{ij}(k,t)-\Pi_i(t)|\leq(1-\sigma^n)^{[\frac{k-t+1}{n}]}$.

The next proof is based on the Lemma 3. Meanwhile, formula (18) can also be written in the form of (19) as

$$\begin{aligned}&\Gamma(k+1)\\=&W(k)\Gamma(k)+\Delta(k)-\alpha_k d_k\\=&\Phi(\mathrm{k},0)\Gamma(0)-\sum_{t=1}^{k+1}\Phi(k,t)\alpha_{t-1}d_{t-1}+\sum_{t=1}^{k+1}\Phi(k,t)\Delta(t-1)\end{aligned} \tag{19}$$

where $\Phi(k,t) = W(k)\cdots W(t)$, $t<k$, $\Phi(k,k) = W(k)$, and $\Phi(k,k+1) = I_N.I_N$ is an identity matrix of size $N\times N$. With consideration of the properties of FDI attacks and referring to Lemma 1, the state error values $\theta_i(k)$ and subgradient $d_k$ satisfy Assumption 4 and 5.

**Assumption 4:** For all $i \in V$, $j \in N_i$, $\theta_i(k)$ satisfies the following attributes:

$$\theta_i(k) \le \theta(k), \lim_{k\to\infty}\theta(k) = 0, \sum_{k=0}^{\infty}\theta^2(k) < \infty. \tag{20}$$

**Assumption 5:** Assume for all participants that the computation of $d_k$ stops after $\overline{k}$, that is, after $\overline{k}$ subgradient is replaced by 0.

Assumption 5 implies that all participants are in a smooth state after $\overline{k}$ iterations and their state values do not change, then one can also obtain that $\Delta_i(k) = 0$. For all $k > \overline{k}$, according to Lemma 2, as $\overline{k}\to\infty$, it can get:

$$\begin{aligned}
&\lim_{k\to\infty}\Gamma(\bar{k}+k)\\
&= \lim_{k\to\infty}\Phi(k,0)\Gamma(0) - \sum_{t=1}^{\bar{k}}\lim_{k\to\infty}\alpha_{t-1}\Phi(\bar{k}+k,t)d_{t-1}\\
&+ \sum_{t=1}^{\bar{k}}\lim_{k\to\infty}\Phi(\bar{k}+k,t)\Delta(t-1)\\
&= [\langle\Pi(0),\Gamma(0)\rangle - \sum_{t=1}^{\bar{k}}\langle\Pi(t),\alpha_{t-1}d_{t-1}-\Delta(t-1)\rangle]1
\end{aligned} \tag{21}$$

It can be found that the limit values of this vector converge to the same value, and the same value is defined as $y(\overline{k})$, it can get

$$y(\bar{k}) = \langle\Pi(0),\Gamma(0)\rangle - \sum_{t=1}^{\bar{k}}\langle\Pi(t),\alpha_{t-1}d_{t-1}-\Delta(t-1)\rangle. \tag{22}$$

Combined with Assumption 5 and (22), the iterative equation for $y(\overline{k})$ can be written as:

$$y(\bar{k}+1) = y(\bar{k}) - \left\langle\Pi(k+1),\alpha_{\overline{k}}d_{\overline{k}} - \Delta(\bar{k})\right\rangle \tag{23}$$

For convenience, replace $\overline{k}$ with $k$. The convergence state of the state values is evaluated by referring to the convex optimal set of [24]. Firstly, for any given $\mu$ and $v$, the set of functions is $C(\mu,\nu) = \left\{q(\lambda)\middle|q(\lambda) = \sum_{i\in V}\Upsilon_i t_i(\lambda)\right\}$, where $\Upsilon_i \ge 0$, $\sum_{i\in V}\Upsilon_i = 1$, $\sum_{i\in V} I\{\Upsilon_i \ge \mu\} = v$, and $I(\cdot)$ is the indicator function. Then define the optimal convex set

$$Y(\mu,\nu) = \cup_{q(x)\in\mathcal{C}(\mu,\nu)}\arg\min_{x\in R} q(x) \tag{24}$$

This proof shows that $\lambda_i(k)$ converges to the intermediate factor $y(k)$, followed by $y(k)$ converging to the convex set $Y(\mu,\nu)$. Note that $Y(\mu,\nu)$ is a convex set when $\mu \ge {r_0}^{-r_0}$ and $\nu = r_1$. Specific parametric properties about $r_0$ and $r_1$ can be found in Ref. [24].

**Lemma 4:** Let $\{a_k\}_{k=0}^{\infty}$, $\{b_k\}_{k=0}^{\infty}$, and $\{c_k\}_{k=0}^{\infty}$ be nonnegative sequences. Suppose that

$$a_{k+1} \le a_k - b_k + c_k, \forall k > 0$$

with $\sum_{k=0}^{\infty} c_k < \infty$. Then $\sum_{k=0}^{\infty} b_k < \infty$ and the sequence $\{a_k\}_{k=0}^{\infty}$ converges to a nonnegative value [29].

**Lemma 5:** $\forall x \in R$ and $\forall k \ge 0$, then the following relation holds:

$$\begin{aligned}
&\left|y(k+1)-\lambda\right|^2\\
&\le \left|y(k)-\lambda\right|^2 + 4H\alpha_k\sum_{j=1}^{n}\Pi_j(k+1)|y(k)-\lambda_j(k)|\\
&- 2\alpha_k\sum_{j=1}^{n}\Pi_j(k+1)(t_j(y(k)) - t_j(\lambda))\\
&+ 2\sum_{j=1}^{n}\Pi_j(k+1)\Delta_j(k)(y(k)-\lambda) + \sum_{j=1}^{n}(\alpha_k d_k - \Delta(k))^2
\end{aligned} \tag{25}$$

Proof: The Lemma 5 can be proved in Appendix.B.

**Lemma 6:** Let $x = \min_{i\in V_i}\lambda_i(0)$, and $X = \max_{i\in V_i}\lambda_i(0)$. For $\forall i \in V_i$, the following inequality can be obtained inequality:

$$\begin{aligned}
&|y(k)-\lambda_i(k)| \le n(1-\sigma^n)^{[\frac{k}{n}]}\max\{|x|,|X|\}\\
&+ nH\sum_{t=1}^{k-1}\alpha_{t-1}(1-\sigma^n)^{[\frac{k-t}{n}]} + 2(\alpha_{k-1}H + \mathrm{M}(k-1))
\end{aligned} \tag{26}$$

Proof: The upper bound on (26) is proved in Appendix.C.

**Lemma 7:** If Assumption 1 holds, one can obtain $\sum_{k=0}^{\infty} c_k < \infty$. And then, one can obtain achieve

$$\lim_{k\to\infty}|y(k)-\lambda_i(k)| = 0 \tag{27}$$

Proof: The Lemma 7 can be proved in Appendix.D.

From Lemma 7, one eventually obtains $\lim_{k\to\infty}\lambda_i(k) = \lim_{k\to\infty}\lambda_j(k) \in Y(\mu,v)$. Thus, the proof of convergence of the algorithm ERCA ends.

## V. SIMULATION RESULTS

This chapter validates the effectiveness of ERCA in an IEEE 39-bus system, which consists of ten generators with $i = 1\sim 10$, and eighteen load consumers with $j = 11\sim 28$. To testify resilient defense strategies against DoS and FDI attacks, nodes 1,2,7,12,17,18,19,21,22,23 and 28 are set as trusted nodes, blue nodes are set to normal nodes, and red nodes 4,10,26 and 27 as nodes infected by FDI attack, communication links $9\leftrightarrow 24$ and $25\leftrightarrow 26$ are considered as being subjected to DoS attacks. The specific network diagram is shown in Figure 1, and all parameter details about generators and load consumers can be found in literature [30]. The case was presented based on $v_4^{\lambda}(k) = 40 * 0.35^k, v_1 0^{\lambda}(k) = 100 * 0.85^k, v_2 6^{\lambda}(k) =$

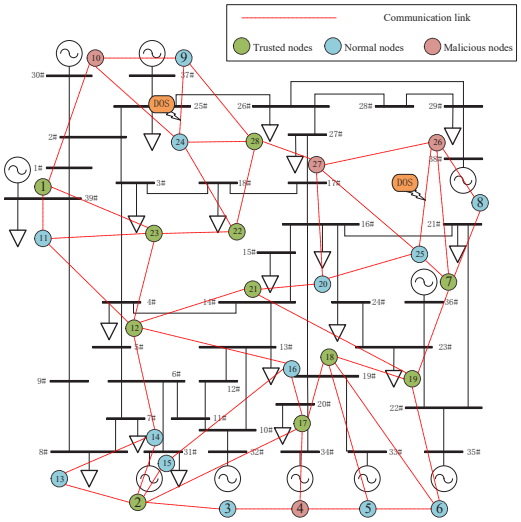



**Fig. 1:** The physical structure and network example of an IEEE 39-bus system.

$30 * 0.25^k, v_1 0^\lambda(k) = 50 * 0.35^k$ to show the effect of FDI attacks and based on $\varphi(9 \leftrightarrow 24, 25 \leftrightarrow 26) = 0.2$ to demonstrate the situation of DoS attacks. The results obtained include two parts: analysis of attack disruption and analysis of resistance strategy results, as shown from V-A to V-B.

### *A. Convergence Analysis under FDI and DoS Attacks*

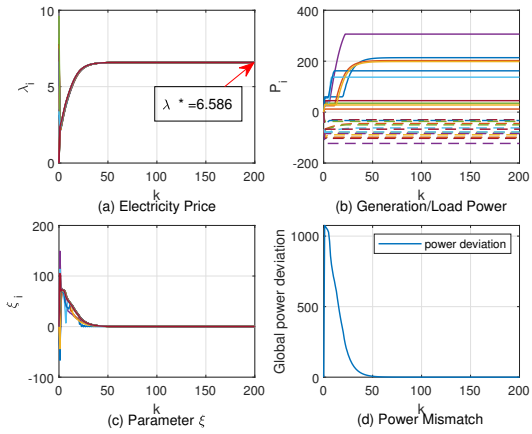



**Fig. 2:** System convergence performance of CEMA without attacks.

According to CEMA in Literature [30], the optimal electricity price and optimal output can be obtained, as well as the error between local and global power generation and load demand, as shown in Figure 2. The electricity price information is $\lambda_i = 6.586$, the power generation and demand distribution are shown in Figure $2(b)$, where the load power is set to negative power. Figure $2(c)$ shows that the local power error gradually approaches 0. Figure $2(d)$ shows that global power error is 0, which means that the equality constraint of Equation 5 are satisfied. Figure $3(a)$, $5(a)$ and $6(a)$ show the performance of the traditional algorithm CEMA under both FDI and DoS attacks. The final electricity prices of each power generation and load unit are shown in Figure $3(a)$. Due to the presence of FDI attacks, the electricity price of the node reached an abnormal peak within 200 iterations, gradually falling back to a convergent value, which could mislead the system to produce incorrect energy management results. Some links are affected by DoS attacks, causing obvious oscillations in the iteration of the node and affecting the convergence state, thus destroying the optimality of the traditional algorithm. As shown in Figure $5(a)$, the fluctuation of electricity price will affect the optimal output of the system. The optimal output of the attacked node fluctuates greatly. Figure 7 shows the trajectory of the mismatch between global power generation and demand, that is, the balance constraint $\sum_{i \in V_G} P_i = \sum_{j \in V_D} P_j$, where can be seen that there is a serious imbalance between supply and demand as a result of FDI and DoS attacks. And Figure $6(a)$ is the local power error, it shows that under the comprehensive effect of attacks, the local power mismatch of the system is unbalanced, which means that the global supply and demand are unbalanced.

### *B. Comparison Analysis with Resistance Strategy*

To prove the optimality of the energy management algorithm amid DoS and FDI attacks, this paper shows the performance of ERCA algorithm. Figures 3, 5, 6 and 7 provide a comparative analysis of DoS and FDI attacks on CEMA and ERCA, demonstrating the superior performance of ERCA. In Figure $3(b)$, prices continue to exhibit significant oscillations due to FDI attacks. While $\lambda_i$ is very close to the optimal price within 200 iterations. Despite the impact of DoS, characterized by packet loss, the incremental cost estimation still converges towards the optimal electricity price. Figure 4 shows the number of packet losses incurred by a node experiencing a DoS attack. Additionally, Figure $5(b)$ presents that the attack has minimal impact on optimal power output under the resilient strategy.

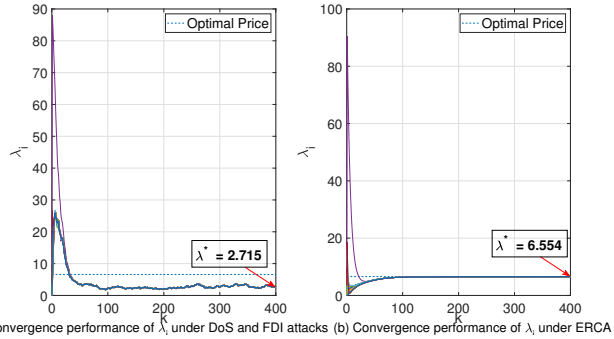



**Fig. 3:** Comparison of convergence performance of $\lambda_i$ between CEMA under attacks and ERCA.

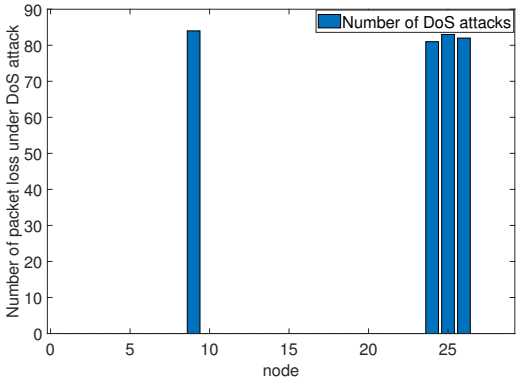



**Fig. 4:** Statistics on the number of DoS attacks on nodes.

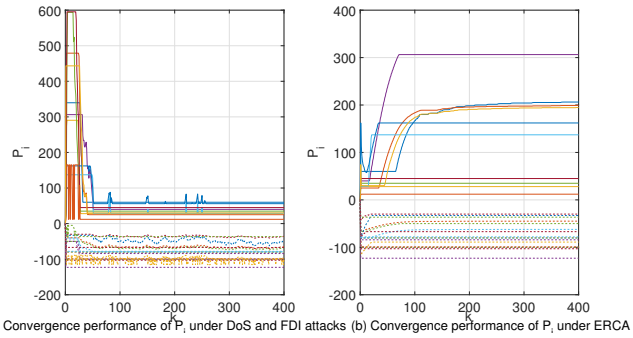



**Fig. 5:** Comparison of convergence performance of $P_i$ between CEMA under attacks and ERCA.

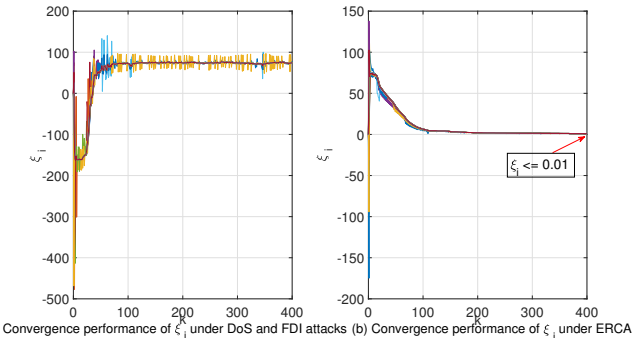



**Fig. 6:** Comparison of convergence performance of $\xi_i$ between CEMA under attacks and ERCA.

From Figure $6(b)$, it can be seen that the proposed ERCA algorithm can effectively eliminate the imbalance error between local power generation and load demand. To better highlight ERCA performance, Figure 7 compares the error between global power generation and load demand imbalance under ERCA,CAMA and CEMA under FDI and DoS attacks. It is evident that the convergence effect of the ERCA algorithm approaches the obtained solution of CEMA and greatly eliminates the impact of attacks. The information sharing in this paper is based on an event-triggered communication mecha-

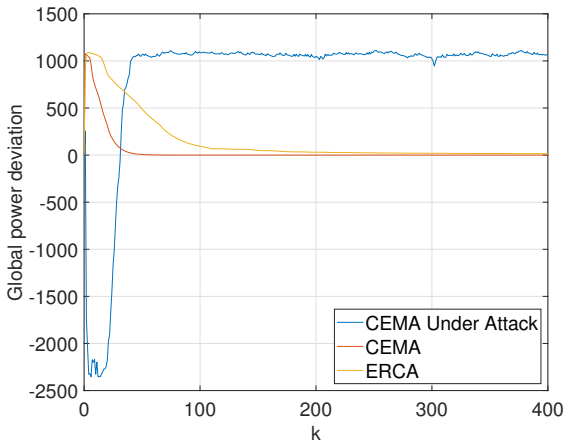



**Fig. 7:** Convergence performance of global power deviation under ERCA.

nism. The proposed mechanism alleviates the communication burden caused by attacks. As shown in Figure 8, compared with traditional communication methods, the event-triggered mechanism greatly reduces the communication frequency of the system. There is no abnormality in the communication frequency of the attacking nodes 4, 10, 26, and 27, which further verifies that the ERCA algorithm mitigates the impact of the attack. The proposed ERCA algorithm in this paper can achieve efficient and secure operation of the system even under cyber attack.

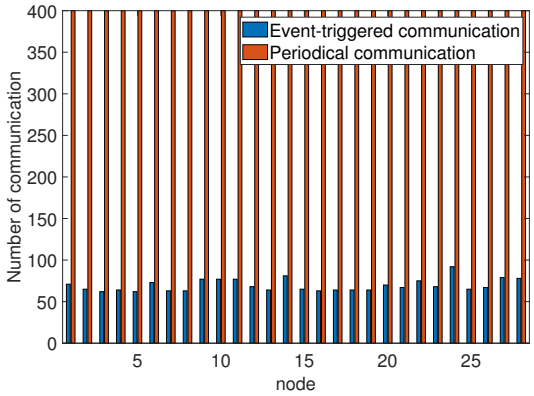



**Fig. 8:** Number of communications.

## VI. CONCLUSION

This paper proposes a resilient consistency algorithm for Cyber-Physical systems when subjected to DoS and FDI attacks, ensuring the security and stability of the power grid. The paper designs models for FDI and DoS attacks, it introduces ACK signals and configures trusted nodes to detect DoS and FDI attacks. Finally, compensation measures based on event-triggering are designed to ensure the secure update of information and guarantee the system's stable operation. Additionally, the theoretical validity of ERCA is verified, and

simulations are conducted to further confirm the effectiveness and superiority of ERCA. The current work focuses on designing resilient strategies tailored to the characteristics of DoS and FDI attacks, and future work will focuse on attacks in Cyber-Physical System and designing resilient distributed strategies with generality.

## ACKNOWLEDGMENT

This work was supported in part by National Natural Science Fund (Grant NO. 61973171, 62293500, 62293505, 52077106 62233010), the Basic research project of leading technology of Jiangsu Province under Grant (BK20202011), National Natural Science Fund of Jiangsu province (BK20211276).

## REFERENCES

[1] H. Zhang, Z. Chen, T. Ye, D. Yue, X. Xie, X. Hu, C. Dou, G. P. Hancke, and Y. Xue, "Security event-trigger-based distributed energy management of cyber-physical isolated power system with considering nonsmooth effects," *IEEE Transactions on Cybernetics*, pp. 1–12, 2023.

[2] Z.-W. Liu, X. Yu, Z.-H. Guan, B. Hu, and C. Li, "Pulse-modulated intermittent control in consensus of multiagent systems," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 47, no. 5, pp. 783–793, 2017.

[3] Z.-W. Liu, G. Wen, X. Yu, Z.-H. Guan, and T. Huang, "Delayed impulsive control for consensus of multiagent systems with switching communication graphs," *IEEE Transactions on Cybernetics*, vol. 50, no. 7, pp. 3045–3055, 2020.

[4] Y. Gao, J. Ma, J. Wang, and Y. Wu, "Event-triggered adaptive fixed-time secure control for nonlinear cyber-physical system with false data-injection attacks," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 70, no. 1, pp. 316–320, 2023.

[5] Y. Chen, D. Qi, H. Dong, C. Li, Z. Li, and J. Zhang, "A fdi attack-resilient distributed secondary control strategy for islanded microgrids," *IEEE Transactions on Smart Grid*, vol. 12, no. 3, pp. 1929–1938, 2021.

[6] X. Cai, F. Xiao, and B. Wei, "Resilient nash equilibrium seeking in multiagent games under false data injection attacks," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 53, no. 1, pp. 275–284, 2023.

[7] H. Zhang, D. Yue, C. Dou, and G. P. Hancke, "Resilient optimal defensive strategy of micro-grids system via distributed deep reinforcement learning approach against fdi attack," *IEEE Transactions on Neural Networks and Learning Systems*, pp. 1–11, 2022.

[8] S. Zuo and D. Yue, "Resilient containment of multigroup systems against unknown unbounded fdi attacks," *IEEE Transactions on Industrial Electronics*, vol. 69, no. 3, pp. 2864–2873, 2022.

[9] H. Guo, J. Sun, and Z.-H. Pang, "Stealthy fdi attacks against networked control systems using two filters with an arbitrary gain," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 69, no. 7, pp. 3219–3223, 2022.

[10] A.-Y. Lu and G.-H. Yang, "Input-to-state stabilizing control for cyber-physical systems with multiple transmission channels under denial of service," *IEEE Transactions on Automatic Control*, vol. 63, no. 6, pp. 1813–1820, 2018.

[11] V. Havlena, P. Matoušek, O. Ryšavý, and L. Holík, "Accurate automata-based detection of cyber threats in smart grid communication," *IEEE Transactions on Smart Grid*, vol. 14, no. 3, pp. 2352–2366, 2023.

[12] Z.-W. Liu, Y.-L. Shi, H. Yan, B.-X. Han, and Z.-H. Guan, "Secure consensus of multiagent systems via impulsive control subject to deception attacks," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 70, no. 1, pp. 166–170, 2023.

[13] J. Liu, e. Gong, L. Zha, E. Tian, and X. Xie, "Interval type-2 fuzzy-model-based filtering for nonlinear systems with event-triggering weighted try-once-discard protocol and cyber-attacks," *IEEE Transactions on Fuzzy Systems*, pp. 1–12, 2023.

[14] J. Liu, E. Gong, L. Zha, X. Xie, and E. Tian, "Outlier-resistant recursive security filtering for multirate networked systems under fading measurements and round-robin protocol," *IEEE Transactions on Control of Network Systems*, vol. 10, no. 4, pp. 1962–1974, 2023.

[15] Z. Lian, F. Guo, C. Wen, C. Deng, and P. Lin, "Distributed resilient optimal current sharing control for an islanded dc microgrid under dos attacks," *IEEE Transactions on Smart Grid*, vol. 12, no. 5, pp. 4494–4505, 2021.

[16] H. Zhang, D. Yue, C. Dou, X. Xie, K. Li, and G. P. Hancke, "Resilient optimal defensive strategy of tsk fuzzy-model-based microgrids' system via a novel reinforcement learning approach," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 34, no. 4, pp. 1921–1931, 2023.

[17] X. Li, C. Jiang, D. Du, W. Li, M. Fei, and L. Wu, "A novel state estimation method for smart grid under consecutive denial of service attacks," *IEEE Systems Journal*, vol. 17, no. 1, pp. 513–524, 2023.

[18] K.-D. Lu and Z.-G. Wu, "Resilient event-triggered load frequency control for cyber-physical power systems under dos attacks," *IEEE Transactions on Power Systems*, vol. 38, no. 6, pp. 5302–5313, 2023.

[19] J. Liu, N. Zhang, L. Zha, X. Xie, and E. Tian, "Reinforcement learning-based decentralized control for networked interconnected systems with communication and control constraints," *IEEE Transactions on Automation Science and Engineering*, pp. 1–12, 2023.

[20] H. Chen, G. Zong, F. Gao, and Y. Shi, "Probabilistic event-triggered policy for extended dissipative finite-time control of mjss under cyber-attacks and actuator failures," *IEEE Transactions on Automatic Control*, vol. 68, no. 12, pp. 7803–7810, 2023.

[21] H. Chen, G. Zong, X. Zhao, F. Gao, and K. Shi, "Secure filter design of fuzzy switched cpss with mismatched modes and application: A multidomain event-triggered strategy," *IEEE Transactions on Industrial Informatics*, vol. 19, no. 10, pp. 10 034–10 044, 2023.

[22] X. Chen, S. Hu, Y. Li, D. Yue, C. Dou, and L. Ding, "Co-estimation of state and fdi attacks and attack compensation control for multi-area load frequency control systems under fdi and dos attacks," *IEEE Transactions on Smart Grid*, vol. 13, no. 3, pp. 2357–2368, 2022.

[23] X.-G. Guo, X. Fan, J.-L. Wang, and J. H. Park, "Event-triggered switching-type fault detection and isolation for fuzzy control systems under dos attacks," *IEEE Transactions on Fuzzy Systems*, vol. 29, no. 11, pp. 3401–3414, 2021.

[24] C. Zhao, J. He, and Q.-G. Wang, "Resilient distributed optimization algorithm against adversarial attacks," *IEEE Transactions on Automatic Control*, vol. 65, no. 10, pp. 4308–4315, 2020.

[25] Y. Kajiyama, N. Hayashi, and S. Takai, "Distributed subgradient method with edge-based event-triggered communication," *IEEE Transactions on Automatic Control*, vol. 63, no. 7, pp. 2248–2255, 2018.

[26] C. Zhao, J. He, P. Cheng, and J. Chen, "Analysis of consensus-based distributed economic dispatch under stealthy attacks," *IEEE Transactions on Industrial Electronics*, vol. 64, no. 6, pp. 5107–5117, 2017.

[27] F. Wang, G. Wen, Z. Peng, T. Huang, and Y. Yu, "Event-triggered consensus of general linear multiagent systems with data sampling and random packet losses," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 51, no. 2, pp. 1313–1321, 2021.

[28] L. Ding, Q.-L. Han, B. Ning, and D. Yue, "Distributed resilient finite-time secondary control for heterogeneous battery energy storage systems under denial-of-service attacks," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 7, pp. 4909–4919, 2020.

[29] L. Su and N. H. Vaidya, "Byzantine multi-agent optimization: Part ii," *ArXiv*, vol. abs/1507.01845, 2015.

[30] C. Zhao, J. He, P. Cheng, and J. Chen, "Consensus-based energy management in smart grid with transmission losses and directed communication," *IEEE Transactions on Smart Grid*, vol. 8, no. 5, pp. 2049–2061, 2017.

## APPENDIX

### A. Proof of Lemma 2

The states of all participants can be divided into three groups: the node state set $D_{ij}(k)$ under DoS attack, the normal node state set $S_i(k)$ and the abnormal state set $F_i(k)$, in which the own state is included in set $S_i(k)$. Since the states in $D_{ij}(k)$ need to be tested for FDI attacks at the same time, the states of set $D_{ij}(k)$ are distributed among the sets $S_i(k)$

and $F_i(k)$. Thus, the state of node $i$ at time $k$ can be described as:

$$\begin{aligned}\lambda_i(k) =& w_{ij}\left(\sum_{j\in S_i(k)}\widetilde{\lambda}_j(k)+\sum_{j\in F_i(k)}\widetilde{\lambda}_j(k)\right)\\ =&\sum_{j\in V}w_{ij}\lambda_j(k)+\sum_{j\in V}w_{ij}\widehat{e}_j(k)+\sum_{j\in S_i(k)}w_{ij}e_i(k)\\ &+\sum_{j\in F_i(k)}w_{ij}\left(\frac{\hat{\lambda}_i^m(k)+\hat{\lambda}_i^M(k)}{2}-\hat{\lambda}_j(k)\right)\end{aligned} \tag{28}$$

According to formula (14), the state error can be described as $\Delta_i(k)=\sum_{j\in V}w_{ij}\widehat{e}_j(k)+\sum_{j\in S_i(k)}w_{ij}e_i(k)+\theta_i(k)+\eta\xi_i(k)+\tau v_i^{\lambda}(k)$, where $\sum_{j\in S_i(k)}w_{ij}e_i(k)$ is the normal state error in the set $D_{ij}(k)$. So formula (14) can be rewritten as $\lambda_i(k+1)=\sum_{j\in V}w_{ij}\lambda_j(k)+\Delta_i(k)-\alpha_k d_k$. Then, since matrix $w_{ij}$ is a row stochastic matrix, formula (19) can be deduced. Besides, those the auxiliary variables satisfy:

$$\sum_{j\in V}w_{ij}\hat{e}_j(k)\le\sum_{j\in N_i}w_{ij}(\|e_j(k)\|)\le L(k-1) \tag{29}$$

where $L(k-1)$ is bounded, then it can obtain that $\hat{e}_i(k)$ is bounded. In the same way, it can obtain that $e_i(k)$ also converges. According to assumption 4 and literature [30], it can obtain that $\theta_i(k)$ and $\eta\xi_i(k)$ are bounded. Thus, it can be deduced that the state error $\Delta_i(k)$ is bounded. ■

### B. Proof of Lemma 5

For any $x\in R$ and any $k\ge 0$, it can obtain:

$$\begin{aligned}&\left|y(k+1)-\lambda\right|^2\\ =&|y(k)-\langle\Pi(k+1),\alpha_k d_k-\Delta(k)\rangle-\lambda|^2\\ =&|y(k)-\lambda|^2-2(y(k)-\lambda)\langle\Pi(k+1),\alpha_k d_k-\Delta(k)\rangle\\ &+|\langle\Pi(k+1),\alpha_k d_k-\Delta(k)\rangle|^2\end{aligned} \tag{30}$$

Combined with Cauchy-Schwarz inequality, it satisfies $\|\Pi(k+1)\|^2\le\sum_{j=1}^{n}\Pi_j(k+1)=1$, then it can obtain:

$$\begin{aligned}&|\langle\Pi(k+1),\alpha_k d_k-\Delta(k)\rangle|^2\\ \overset{a}{\le}&\|\Pi(k+1)\|^2\|\alpha_k d_k-\Delta(k)\|^2\overset{b}{\le}\|\alpha_k d_k-\Delta(k)\|^2\\ =&\sum_{j=1}^{n}(\alpha_k d_k-\Delta(k))^2\end{aligned} \tag{31}$$

On the basis of the second term on the right of formula (30), the following inequality can be deduced:

$$\begin{aligned}&-2(y(k)-\lambda)\langle\Pi(k+1),\alpha_k d_k-\Delta(k)\rangle\\ &\le 4H\alpha_k\sum_{j=1}^{n}\Pi_j(k+1)(y(k)-\lambda_j(k))\\ &-2\alpha_k\sum_{j=1}^{n}\Pi_j(k+1)(t_j(y(k))-t_j(\lambda))\\ &+2\sum_{j=1}^{n}\Pi_j(k+1)\Delta_j(k)(y(k)-\lambda)\end{aligned} \tag{32}$$

The inequality satisfies the condition that $t_j(\cdot)$ is L-Lipschitz continuous for each $j\in V$. ■

### C. Proof of Lemma 6

For $k>0$, formula (19) can be rewritten as:

$$\begin{aligned}\Gamma(k)=&\Phi(\mathrm{k}\ -1,0)\Gamma(0)-\sum_{t=1}^{k}\Phi(k-1,t)\alpha_{t-1}d_{t-1}\\ &+\sum_{t=1}^{k}\Phi(k-1,t)\Delta(t-1)\end{aligned} \tag{33}$$

Then, each $\lambda_i(k)$ can be calculated as:

$$\begin{aligned}\lambda_i(k)=&\sum_{j=1}^{n}\Phi_{ij}(k-1,0)\lambda_j(0)\\ &-\sum_{j=1}^{n}\sum_{t=1}^{k}\Phi(k-1,t)(\alpha_{t-1}d_j(t-1)-\Delta_j(t-1))\end{aligned} \tag{34}$$

Thus, formula (22) can be written as $y(k)=\sum_{j=1}^{n}\Pi_j(0)\lambda_j(0)-\sum_{j=1}^{n}\sum_{t=1}^{k}\Pi_j(t)(\alpha_{t-1}d_j(t-1)-\Delta_j(t-1))$. According to formula (33) and (34), it can obtain:

$$\begin{aligned}&|y(k)-\lambda_j(k)|\le|\sum_{j=1}^{n}(\Pi_j(0)-\Phi_{ij}(k-1,0))|\lambda_j(0)\\ &+\sum_{j=1}^{n}\sum_{t=1}^{k}(\Phi_{ij}(k-1,t)-\Pi_j(t))(\alpha_{t-1}d_j(t-1)-\Delta_j(t-1))\end{aligned} \tag{35}$$

For the first term of the second equation of formula (30), it can obtain:

$$\begin{aligned}&|\sum_{j=1}^{n}(\Pi_j(0)-\Phi_{ij}(k-1,0))|\lambda_j(0)\\ \le&\sum_{j=1}^{n}|\Pi_j(0)-\Phi_{ij}(k-1,0)||\lambda_j(0)|\\ \le&n(1-\sigma^n)^{[\frac{k}{n}]}\max\{|x|,|X|\}\end{aligned} \tag{36}$$

In addition, since the condition $\Phi(k-1,k)=I$ holds, the second term in formula (34) satisfies:

$$\begin{aligned}
&\sum_{j=1}^{n}\sum_{t=1}^{k}(\Phi_{ij}(k-1,t)-\Pi_j(t))(\alpha_{t-1}d_j(t-1)-\Delta_j(t-1))\\
&\le\sum_{t=1}^{k-1}(\sum_{j=1}^{n}|\Phi_{ij}(k-1,t),\Pi_j(t)||\alpha_{t-1}||d_j(t-1)|\\
&+\sum_{j=1}^{n}\Pi_j(k)|(\alpha_{k-1}(d_i(k-1)-d_j(k-1))|\\
&+\sum_{j=1}^{n}|\Delta_j(k-1)-\Delta_i(k+1)|\\
&\le nH\sum_{t=1}^{k-1}\alpha_{t-1}(1-\sigma^n)^{[\frac{k-t}{n}]}+2(\alpha_{k-1}H+\mathrm{M}(k-1))
\end{aligned}\tag{37}$$

where $\mathrm{M}(k)$ is the upper bound of $\sum_{j=1}^{n}\Delta_j(k)$. Combined with formula (35), (36) and (37), then Lemma 6 holds. ■

*D. Proof of lemma 7*

Let $\lambda^*\in Y(\mu,\nu)$. According to Lemma 4, it can obtain:

$$\begin{aligned}
&\left|y(k+1)-\lambda^*\right|^2\\
&\le\left|y(k)-\lambda^*\right|^2+4H\alpha_k\sum_{j=1}^{n}\Pi_j(k+1)|y(k)-\lambda_j(k)|\\
&-2\alpha_k\sum_{j=1}^{n}\Pi_j(k+1)(t_j(y(k))-t_j(\lambda^*))\\
&+2\sum_{j=1}^{n}\Pi_j(k+1)\Delta_j(k)(y(k)-\lambda^*)+\sum_{j=1}^{n}(\alpha_k d_k-\Delta(k))^2
\end{aligned}\tag{38}$$

Here, some variables can be defined as follows:

$$\begin{aligned}
a_k&=\left|y(k)-\lambda^*\right|^2\\
b_k&=2\alpha_k\sum_{j=1}^{n}\Pi_j(k+1)(t_j(y(k))-t_j(\lambda^*))\\
c_k&=4H\alpha_k\sum_{j=1}^{n}\Pi_j(k+1)|y(k)-\lambda_j(k)|\\
&+2\sum_{j=1}^{n}\Pi_j(k+1)\Delta_j(k)(y(k)-\lambda^*)+\sum_{j=1}^{n}(\alpha_k d_k-\Delta(k))^2
\end{aligned}\tag{39}$$

Then, it is obvious that $a_k\ge 0$ and $c_k\ge 0$. Thus, it can deduce that $b_k\ge 0$. The first item of the $c_k$ satisfies:

$$\begin{aligned}
&\sum_{j=1}^{n}\Pi_j(k+1)|y(k)-\lambda_j(k)|\le n(1-\sigma^n)^{[\frac{k}{n}]}\max\{|x|,|X|\}\\
&+nH\sum_{t=1}^{k-1}\alpha_{t-1}(1-\sigma^n)^{[\frac{k-t}{n}]}+2(\alpha_{k-1}H+\mathrm{M}(k-1))
\end{aligned}\tag{40}$$

Then, it can be further deduced as:

$$\begin{aligned}
&\sum_{k=0}^{\infty}4H\alpha_k\sum_{j=1}^{n}\Pi_j(k+1)|y(k)-\lambda_j(k)|\\
&\le\sum_{k=0}^{\infty}4H\alpha_k n(1-\sigma^n)^{[\frac{k}{n}]}\max\{|x|,|X|\}\\
&+\frac{nH}{2}\sum_{k=0}^{\infty}\sum_{t=1}^{k-1}\alpha^2(k)(1-\sigma^n)^{[\frac{k-t}{n}]}+2\sum_{k=0}^{\infty}(\alpha_{k-1}H+\mathrm{M}(k-1))\\
&+\frac{nH}{2}\sum_{k=0}^{\infty}\sum_{t=1}^{k-1}\alpha^2(k-1)(1-\sigma^n)^{[\frac{k-t}{n}]}<\infty
\end{aligned}\tag{41}$$

On the basis of Assumption (5), the third item of the $c_k$ satisfies:

$$\sum_{k=0}^{\infty}\sum_{j=1}^{n}(\alpha_k d_k-\Delta(k))^2=\sum_{k=0}^{\overline{k}}\sum_{j=1}^{n}(\alpha_k d_k-\Delta(k))^2<\infty\tag{42}$$

Similarly, the second term can be deduced as:

$$\begin{aligned}
&2\sum_{k=0}^{\infty}\sum_{j=1}^{n}\Pi_j(k+1)\Delta_j(k)(y(k)-\lambda^*)\\
&=2\sum_{k=0}^{\overline{k}}\Delta(k)\sum_{j=1}^{n}\Pi_j(k+1)(y(k)-\lambda^*)<\infty
\end{aligned}\tag{43}$$

Hence, it satisfies that $\sum_{k=0}^{\infty}c_k<\infty$, then it can deduce that $\sum_{k=0}^{\infty}b_k<\infty$ as follows:

$$\sum_{k=0}^{\infty}b_k=\sum_{k=0}^{\infty}2\alpha_k\sum_{j=1}^{n}\Pi_j(k+1)(t_j(y(k))-t_j(\lambda^*))<\infty\tag{44}$$

It follows that $y(k)$ converges with $k$. Suppose that $\lim_{k\to\infty}y(k)\notin Y(\mu,v)$, then formula (45) can be obtained.

$$\lim_{k\to\infty}\sum_{j=1}^{n}\Pi_j(k+1)t_j(y(k))-\sum_{j=1}^{n}\Pi_j(k+1)t_j(\lambda^*)\neq 0\tag{45}$$

Then, it is obvious that formula (45) contradicts with formula (44), it can be deduced that $\lim_{k\to\infty}y(k)\in Y(\mu,v)$. So, it can be deduced that $y(k)$ is the limit of $\lambda_i(k)$. Thus if $k\ge\overline{k}$, $y(k)=y(\overline{k})$, it can be obtain:

$$\lim_{k\to\infty}|y(k)-\lambda_i(k)|=0\tag{46}$$

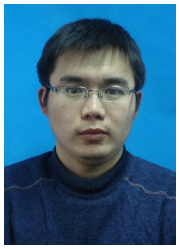
Hence, it can be proved that Lemma 7 holds. ■

**Huifeng Zhang** (M'16-SM'22) received Ph.D. degree from Huazhong University of Science and Technology, Wuhan, China, in 2013. From 2014 to 2016, he was a Post-Doctoral Fellow with the Institute of Advanced Technology, Nanjing University of Posts and Telecommunications, Nanjing, China. From 2017 to 2018, He was granted as visiting research fellow by China Scholarship Council to study in Queens University Belfast and University of Leeds, UK. He is currently an Associate Professor at the Institute of Advanced Technology, Nanjing University of Posts and Telecommunications, Nanjing, China. His current research interest includes electrical power management, optimal operation of power system, distributed optimization, and multi-objective optimization.

**Zhuxiang Chen** is currently pursuing the M.Sc. degree in control science and engineering with Nanjing University of Posts and Telecommunications, Nanjing, China. Her research interests include resilient security of power system and distributed optimization.

**Chengqian Yu** is currently pursuing the M.Sc. degree in control science and engineering with Nanjing University of Posts and Telecommunications, Nanjing, China. His research interests include event-triggered control and distributed optimization.

**Dong Yue** (SM'08-F'20) received the Ph.D. degree from the South China University of Technology, Guangzhou, China, in 1995. He is currently a Professor and the Dean with the Institute of Advanced Technology, Nanjing University of Posts and Telecommunications, Nanjing, China, and also a Changjiang Professor with the Department of Control Science and Engineering. His current research interests include analysis and synthesis of networked control systems, multiagent systems, optimal control of power systems, and internet of things. Prof. Yue is currently an Associate Editor of the IEEE Control Systems Society Conference Editorial Board and the International Journal of Systems Science.



**Xiangpeng Xie** (M'16-SM'23) received the B.S. and Ph.D. degrees from Northeastern University, Shenyang, China, in 2004 and 2010, respectively, both in engineering. From 2012 to 2014, he was a Post-Doctoral Fellow with the Department of Control Science and Engineering, Huazhong University of Science and Technology, Wuhan, China. He is currently a Professor with the Institute of Advanced Technology, Nanjing University of Posts and Telecommunications, Nanjing, China. His current research interests include fuzzy modeling and control synthesis, state estimations, optimization in process industries, and intelligent optimization algorithms.

**Gerhard P. Hancke** (M'88-SM'00-F'16) received the B.Sc. and B.Eng. degrees, in 1970, and the M.Eng. degree in Electronic Engineering, in 1973, from the University of Stellenbosch, South Africa, and the Ph.D. degree from the University of Pretoria, South Africa, in 1983. He is a Professor with the University of Pretoria, South Africa and recognized internationally as a pioneer and leading scholar in industrial wireless sensor networks research. He initiated and co-edited the first Special Section on Industrial Wireless Sensor Networks in the IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS in 2009 and the IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS in 2013. Prof. Hancke has been serving as an Associate Editor and Guest Editor for the IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, IEEE ACCESS, and previously the IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS. Currently, he is a Co-Editor-in-Chief for the IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS.